CHAPTER 5

DIGITAL INFORMATIONAL SYSTEMS SECURITY PROCEDURES

5-1. General

The use of the C4I system, telecommunications networks, and other AIS is available throughout the DOD. These systems and their databases play critical roles in operation, C4I, finance, personnel, and logistics missions. The systems' growing connectivity and the wealth of valuable information they process and store make them attractive targets for compromise of data, deception/corruption of data, disruption of system operation, or actual physical destruction of equipment. They are faced with threats that are genuine, worldwide in origin, technically diverse, multifaceted, and rapidly growing.

5-2. Communications Security

The present and ever-increasing dependence upon the AIS within the Army mandates that the security of *all* components (the information generated by and the systems that generate the information, the signal that transmits the information, and all processing systems) be protected. Risk management should be applied to all systems, to include classified systems as well as unclassified and/or sensitive systems. Threats to US systems can occur in two distinct areas, electronic warfare and computer intrusion. Both are part of command and control warfare and may occur independently or at the same time.

5-3. Warfighters Architecture Requirements

The Army's enterprise strategy focuses on three warfighter crucial architectures (see Appendix A).

a. The goal of the current security architecture is to ensure sensitive information and assets are protected throughout the continuum of military operations.

b. Earlier security systems did not meet the requirements for flexibility, accountability, and interoperability. Security policies and procedures are now developed to satisfy current requirements.

c. It is imperative that users exchanging information know that the data is authentic; that it is sent by valid users; and that it is not available to unauthorized personnel. Current and future security architecture must protect the confidentiality, integrity, and availability of information that is created, processed, stored, and communicated. Threats to the AIS are multifaceted in nature. They can come from a variety of sources ranging from an accidental intrusion to a deliberate military attack. The degree of acceptable risk in the assessment process is directly proportionate to the data's sensitivity, criticality, and perishability when compared to the threat.

5-4. Current Security Policy

The current security policy for the tactical packet network (TPN) mandates all hardware be accredited for secret high operation. The exception to this policy is the tunneling of sensitive but unclassified (SBU) information via in-line network encryption (currently the network encryption systems), through the deployed TPN. The typical configuration calls for the use of firewalls at gateway points between network types and high assurance guards between the secret Internet protocol router network and the nonclassified Internet protocol router network.

a. The National Security Agency (NSA) is developing a set of solutions to provide secure interoperability for the Defense Information Infrastructure (DII) and the Defense Information System Network (DISN) (a subset of DII). (The area common-user system and the TPN are subsets of DISN.) The NSA solution, the Multilevel Information Systems Security Initiative (MISSI), is expected to provide the security services required by the WIN security policy through all transitional phases. The MISSI products will provide the following security services:

(1) *Data integrity* (*verification that data has not been modified in transmission or during computer processing*). Currently no widely used capability exists to accomplish this with electronic mail (E-mail) or with the message traffic (hard or soft copy). This is a new requirement.

(2) *Identification and authentication* (*I&A*) (*verification of the transaction originator*). This is similar to using a personal identification number (PIN) on a bankcard. Current procedures require system administrators and information system security officers to issue user identification (USERID) and passwords. The potential exists for a release authority to give his USERID and password to an unauthorized person. The same potential exists when using crypto cards and PINs.

(3) *Nonrepudiation* (*proof of participation by both sender and receiver in a transaction*). Current capabilities allow confirmation when the user receives or reads E-mail. However, the Army uses many E-mail software packages that do not have this capability.

(4) *Data confidentiality* (*data privacy with encryption during transmission or computer processing*). This includes encrypting text before transmission or the separation of data during processing. Using bulk data encryption and limiting network access meets this requirement. The secure telephone unit (STU) keys provide this capability for voice traffic over commercial networks.

(5) *Access control* (*ensuring that data transmission or computing processing systems are not denied authorized users*). Firewalls prevent the unauthorized access while the secure mail guard provides for multilevel security E-mail exchange. This capability is not fully utilized in garrison environments and is not currently deployed.

b. A MISSI building block approach is used to develop products that stay current with evolving security requirements and technology (Figure 5-1). Product categories are as follows:

(1) *Workstation security products*. These products include crypto cards and their associated crypto-ready applications that perform workstation security services.

(2) *Crypto-ready applications*. An evolving set of commercially available user software packages that call up the crypto security services.

(3) *System/enclave security products*. These products typically reside at the enclave boundary and provide access control and/or encryption services to external networks.

(4) *Secure computing products*. These products are high trust computer operating systems and application programs that contain features and assurances that support information sensitivity labels. They also prevent the deliberate or accidental release of information to unauthorized users. These capabilities enhance security in the local enclave. These capabilities currently exist in networks that use USERID and system-level passwords.

(5) *Network security management products*. These products support the security management of the network and perform services such as electronic key generation and distribution, issuing user certificates, maintaining user directories, and revoking user privileges.

(6) *Voice security products*. The MISSI does not provide voice security products. However, MISSI technology will be used in the secure telephone equipment (STE). The STE will be compatible with existing STU-IIIs and will replace existing KY-68s. Additionally, the near-term digital radio may use personal computer (PC) crypto cards and embedded cryptographic modules.

c. Prior to fielding WIN upgrades, developers will employ security tools (see FM 100-6) to identify system vulnerabilities and apply countermeasures. Access controls, MISSI security services, and encryption will be used to protect the confidentiality and integrity of the data passed. These tools will also be used at network entrances to isolate segments and detect intrusion. Once detected, countermeasures (including tracing and exploitation) will minimize the impact of the intrusion.

5-5. Midterm Programs and Initiatives

The midterm design will replace network encryption systems with a guard and add a crypto card to support Defense Message System (DMS) and guard fractions.

a. The following security initiatives and capabilities will be implemented as they become available for the majority of systems to support the evolution toward the WIN infrastructure:

(1) Provide a standard technique for “producer-to-consumer” protection of services in the SBU environment (for example, E-mail services, file transfer and storage, and video services). The MISSI security products implement the approved Army standards for SBU-level security.

(2) Integrate initial user account-level security management capabilities into the security architecture. The DMS Phase I delivers security management with a certificate authority workstation (CAW) user agent infrastructure for DMS accounts.

(3) Provide network component-level access controls and user-level distributed I&A services. Using a PC crypto card is the approved Army standard network access control technique and supports log-on and authentication services.

(4) Provide multilevel separation of nonsensitive, SBU, and SECRET information processed over one network environment. This is currently accomplished using in-line network encryptors (INE). The objective security architecture provides trusted guard functionality to allow multilevel operations.

NETWORK

IN-LINE NETWORK ENCRYPTORS: These provide packet encryption at the network level to cryptographically separate users/enclaves.

HIGH ASSURANCE GUARDS: The high assurance guards mediate the exchange of information between systems operating at different security levels. They guard enclaves from malicious attacks and permit/restrict information flow in accordance with security policy.

FIREWALLS: Mediates the exchange of information between systems operating at similar security levels.

SERVICE

TERMINAL

SECURE COMPUTING: This is trusted computing operating systems and application programs.

FORTEZZA FAMILY: These personal computer cryptographic cards contain a variety of algorithms that support MISSI operations between network and terminal devices.

SYSTEMS

INTEGRATED NETWORK SECURITY MANAGEMENT

Figure 5-1. Multilevel information systems security initiative building blocks.

(5) Provide protected interconnection with, and interface to, the Internet. Firewall technology, in conjunction with a crypto card-based I&A, is a proposed way to protect against intrusion from the Internet.

(6) Provide continued separation and protection for TOP SECRET (TS) and sensitive compartmented information. Dedicated intelligence networks or subchannels on existing communications carriers will use INE technology to ensure separation.

(7) Provide secure voice compatibility and interoperability between analog and emerging digital voice communications. Secure telephone equipment, when fielded, will provide compatibility and interoperability with STU in voice mode.

(8) Provide compatible and interoperable cryptography between voice and data systems.

(9) Provide initial common security management infrastructure for end-system and network security products. A common security management infrastructure will support network security and STE. An initial security association management protocol will be available that uses common security labels, a security management information base, and security audit tool applications.

(10) Provide cryptographic security products that support multimedia information processing. High-speed "key agile" encryptors will be developed to support asynchronous transfer mode environments.

(11) Provide end-system security products that are compatible with projected end-system platforms.

(12) Provide compatible interfaces between tactical and garrison C2 environments. Tactical bridges will be provided through the integrated tactical-strategic data network employing MISSI products.

b. The MISSI is an evolutionary initiative with products delivered as available. Each new release of MISSI products will address the system security objectives of improved performance levels and progressively higher assurance. The MISSI products include—

(1) *In-line network encryptors*. These products typically reside at the boundary between local and wide area networks and provide highly robust encryption and access control services. For the near-term security architecture, INEs are used for tunneling and trunk security. For the midterm and objective security architecture, INEs may be used for trunk security.

(2) *Workstation products*. These products reside at individual workstations and provide writer-to-reader security services, intrusion detection, virus detection, and so forth. When used as recommended and in combination with trusted operating systems, application programs, and guard functions, these products may provide multilevel security network solutions.

(3) *Firewalls and secure server products*. A firewall is a set of components that control access between networks. Server products typically reside on the local network boundary as a guard. They can also reside within the local network to provide common security services for applications such as high-low guards, files services, and database management. Examples are the tactical guard and the high assurance guard (HAG); either could be equipped with a data encrypting capability.

(4) *Security management services*. These encompass such security measures as cryptographic keying, access control, authentication, and using passwords. These services include—

(*a*) The CAW, which will reside on the local area network and provide security support for the provision of such capabilities as digital signatures, cryptographic key, and access control permissions.

(*b*) Rekey managers that work in conjunction with the electronic key management system and provide cryptographic rekey support for security products.

(*c*) Audit managers, which provide support for the collection and analysis of security relevant auditable events associated with security products. An example of an auditable event is a repeated failed user log-in.

(*d*) Directories, which provide a repository for public security information essential for global message addressing. An example is the public part of a user's digital signature.

(*e*) Mail list agents, which are employed by messaging systems when a message is sent to many recipients to add security.

(5) The STE will allow transition from a primarily analog environment to a fully digital environment. It builds on the need for a secure voice terminal capable of interfacing with and using the enhanced features and capabilities of the digital infrastructure. Interfaces allow both tactical and strategic digital circuit switching to occur. The STE will offer backwards compatibility and compliance with the integrated service digital network standards for basic rate interface. It will provide high quality digital performance for secure and nonsecure voice and data operations. Security migration will allow for the capabilities to support I&A of individual users that allow voice, data applications, voice conferencing control, and video-conferencing greater security control. Interfaces to both integrated service digital network and switched 56 kilobytes per second digital public switched telephone services will allow both tactical and strategic digital circuit switching to occur.

5-6. Objective Environment

a. The following high-level security objectives represent the target capabilities for the objective security architecture:

(1) Protect and share all levels of security with firewalls and HAGs.

(2) Authenticate access through firewalls and HAGs.

(3) Secure network transactions.

(4) Establish information domains for all functional areas (for example, C2, intelligence, administrative, finance, and so forth).

(5) Institute global, dynamic management for all domains.

(6) Assure availability of service and share security technology with service suppliers.

b. Unlike the midterm architecture that concentrated on a single digitized division, the objective architecture will transition a corps at a time until all are upgraded. This will require an evolutionary process of incorporating security products, policies, and procedures as they are accepted into the Army architecture.

5-7. Multilevel Information Systems Security Initiatives, Secret to Sensitive, but Unclassified Configuration

a. Workstations equipped with crypto cards have writer-to-reader protection for data sharing between the SBU enclaves through unclassified networks. However, possibly in the midterm, legacy trusted vice public networks will be used. During the midterm, the introduction of the HAG enables secret enclaves to exchange SBU data with SBU enclaves and secret enclaves to exchange secret data through unclassified networks. A CAW will be required in the objective architecture. The CAW will provide the network security management for MISSI. The CAW software will include certificate management, directory user agent, DMS user agent, administrative directory user agent, and simple mail transfer.

b. The objective architecture will include crypto cards with both Type I and Type H algorithms and can interoperate from unclassified up to the TS-sensitive compartmented information level. Sometime between the midterm and objective architecture, the legacy secret-level backbone may transition to an unclassified network.

c. Future MISSI capabilities will incorporate future technologies and communications media such as the synchronous optical network and the broadband integrated service digital network. The security management capabilities from earlier solution sets will receive enhancements to provide higher performance in support of large-scale networks, such as the global grid.

d. Specific software and hardware mechanisms will be required to provide the security services in the objective architecture. Crypto cards perform key storage, encryption, decryption, digital signature, and verification of digital signatures. The secure network server for the MISSI configuration is a HAG. The HAG will provide multilevel security functionality in the objective architecture. It will contain multiple functions including mail applications, file transfer protocol, and remote log-in capability. The security policy programmed into the HAG will determine allowable traffic flows. A CAW will be required in the objective architecture. The CAW will provide the network security management for MISSI. The CAW software will include certificate management, directory user agent, DMS user agent, administrative directory user agent, and the simple mail transfer protocol.

5-8. Standardization of Information Operations Security Responsibilities During Joint and Coalition Operations

Standardization of information operations security responsibilities during Joint military and coalition forces is—

- Achieved through international forums in accordance with policy and procedures of the Chairman of Joint Chiefs of International Military Rationalization, Standardization, and Interoperability between the US and its allies and other friendly nations.

- Policy enhancing US military forces to communicate and share data and information with each other and their allies/coalition members.

Areas of particular concern for compatibility and commonality include command, control, communications, and computers (C4) and automated information systems, battlefield surveillance systems, target designation systems, target acquisitions systems, and communications security hardware and software systems.

a. *Chairman, Joint Chiefs of Staff Responsibilities.*

(1) The Chairman, Joint Chiefs of Staff (CJCS) functions within the chain of command by transmitting to the combatant commanders the orders of the President and the Secretary of Defense. The CJCS coordinates all communications in matters of Joint interest addressed to the combatant commanders by other authority.

(2) The Chairman operates the National Military Command System (NMCS) for the Secretary of Defense to meet the needs of the NCA and establishes operational policies and procedures for all components of the NMCS and ensures their implementation.

(3) General operational responsibility for the nuclear command, control, and communications (C3) system lies with the CJCS. The nuclear C3 system is centrally directed through the Joint Staff. The nuclear C3 system supports Presidential nuclear C2 and NCA C2 of the combatant commands in the areas of integrated tactical warning and attack assessment, decision making, decision dissemination, and force management and report back.

b. *Combatant Commander Responsibilities.* Combatant commanders—

(1) Submit C4 system requirements for Joint operations within the scope of their missions and functions to the CJCS. They also provide information copies of the correspondence to the other Services, and defense agencies. This submission will include requirements for CJCS-controlled transportable C4 assets, when such requirements are not satisfied by normal military department or military service processes.

(2) Collect, provide comments on, and forward to the CJCS the requirements applicable to Joint operations for all C4 equipment. The requirements are generated by subordinate operational commands and are submitted directly to the military departments or Services. The DISN/C4 resources must be validated at the combatant commander level.

(3) Report to the CJCS incompatibilities or lack of interoperability among C4 systems and between tactical systems and the DISN.

(4) Test the C4 systems' portions of appropriate OPLANs periodically as a part of a CJCS-sponsored or command-sponsored exercise. These tests will identify unresolved issues, verify operational procedures and interoperability, and provide Joint training.

(5) Ensure that Service components and subordinate unified commands submit requirements for all C4 systems applicable to Joint operations through the combatant commanders to the military departments or Services in accordance with procedures in effect.

5-9. Connectivity to the Sustaining Base

a. Throughout all force projection stages, a paramount need exit for a signal support means to transport information from the sustaining base power projection platform at CONUS installations, through strategic gateways, to forward deployed units. The signal support mission-essential tasks to project and construct the infosphere are to—

- Link the force to the infosphere to achieve seamless global connectivity.

- Transport information with broadband, high-capacity systems, optimizing satellites and terrestrial signal support, to connect CONUS, installation sustaining base, and Joint operational areas.

- Reach back through strategic entry points to power projection platforms and information infusion centers.

- Extend the communication range of battle command operations centers and fighting platforms by providing C4 for mobile operations.

b. The signal IO support mission-essential tasks are to—

- Digitize, compress, and broadcast multimedia battle command information in five categories using increased bandwidth, high-efficiency transport systems. The multimedia categories control, monitor, alert, inquire, and explore critical information.

- Encrypt and provide multilevel information security.

- Manage information networks with smart software that dynamically allocates throughput capacity on demand and then routes and disseminates information.

- Display via Army Battle Command System (ABCS), a three-dimensional, interactive, knowledge-based, relevant common picture.

c. Medical unit commanders request assistance from the supporting signal unit to obtain connectivity with the CONUS sustaining base. Information on message transmission security and information on security levels for various types of wire, wireless, digital, video, and satellite linkages are provide in the signal operating instructions. Also, this information may be obtained from the supporting signal unit.